

The Honorable Thomas S. Zilly

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STRIKE 3 HOLDINGS, LLC, a
Delaware corporation,

Plaintiff,

v.

JOHN DOE, subscriber assigned IP
address 73.225.38.130,

Defendant.

No. 2:17-cv-01731-TSZ

**DECLARATION OF PATRICK
PAIGE**

I, **PATRICK PAIGE**, declare and state as follows:

1. I am a Member of Computer Forensics, LLC and have been retained by Strike 3 Holdings, LLC as a Computer Forensics expert in the above captioned matter.

2. If called as a witness I could testify competently to the matters set forth herein of my own personal knowledge.

3. My *curriculum vitae* ("CV") is attached as Exhibit A.

4. I am an expert in the field of computer forensics. I have testified as a fact and expert witness on numerous occasions in the field of computer forensics in both trial-level and appellate proceedings before state, federal, and military courts in Florida, California, Indiana, New Jersey, New York, and Pennsylvania.

1 5. No court has ever refused to accept my testimony on the basis that I was not
2 an expert in computer forensics.

3 6. I submit this declaration in support of Plaintiff's Supplement in Response to
4 Defendant's Motion for Summary Judgment (hereinafter referred to as "Plaintiff's
5 Supplement").

6 7. I reviewed the Court's September 19, 2019 Order ("Court's Order" or
7 "Order") in this case. The Order states that "Plaintiff may designate one expert to examine
8 [Defendant's] 'imaged' hard drive" but that the examination "shall be limited to searching
9 for existing and/or deleted files matching the hash values set forth in Exhibit A to the
10 Complaint, docket no. 1." Dkt. No. 182. The Court's Order also instructed that Plaintiff's
11 expert "may not search for or view any other materials on the 'imaged' hard drive, including
12 any items protected by attorney-client or work-product privilege." *Id.*

13 8. After carefully reviewing this Order, I determined that I am unable to craft an
14 examination protocol that would confirm the presence or absence of "files matching the hash
15 values set forth in Exhibit A to the Complaint[,] while simultaneously complying with the
16 Order's limitations.

17 9. To explain, the Order permits Plaintiff to only search for the hash values listed
18 in Exhibit A to Plaintiff's Complaint ("Exhibit A Hashes").

19 10. The Exhibit A Hashes are simply "Info Hashes." An Info Hash is a hash value
20 of specific data contained within a .torrent file. The "Info Hash" is the data that the BitTorrent
21 protocol uses to identify and locate the desired file (in this case, the desired file is the
22 respective file for the infringing motion pictures that were the subject of the action) across
23 the BitTorrent network.

24 11. Since each Info Hash is made of up of specific information inside of a .torrent
25 file, searching for the Exhibit A Hashes necessarily entails a specific process: it requires
26 searching *within* all .torrent files on a computer.

1 12. Thus, in order for me (or any expert) to properly search for the Exhibit A
2 Hashes on Defendant's hard drive, I would need to take the following steps

- 3 • First, I would use AXIOM forensic software to locate all the .torrent files on
4 the hard drive.
- 5 • Second, I would export the located .torrent files out of the hard drive image.
6 Exporting entails taking the .torrent files and copying them onto a third-party
7 computer.
- 8 • Third, I would run the exported .torrent files through an open source software
9 called Torrent Hash Extractor¹ (or, in the alternative, any other software
10 designed to extract the hashes within a .torrent file) which allows me to obtain
11 and view the Info Hash for each .torrent file.
- 12 • Finally, I would manually compare the Info Hashes to the Exhibit A Hashes
13 to see if any matched.

14 13. This is the only method I know of which would allow me to conduct a search
15 for the Info Hashes listed in Exhibit A. Michael Yasumoto's Expert Report states that he
16 "compared the SHA1 hash [...] and none of the videos examined on defendant's computer
17 were a hash match for the videos listed in Exhibit [A]." *See* Dkt. No. 175-10, at 5. But, since
18 the Exhibit A Hash are the hash values of specific data contained within the .torrent files (and
19 not the hash values to the infringing movie files themselves) Mr. Yasumoto's examination
20 would not have yielded evidence whether or not the .torrent files are on the computer.

21 14. Performing this examination protocol – the only way to search Defendant's
22 hard drive for the Exhibit A Hashes– would, in my opinion, violate the Court's Order.

23 15. Indeed, searching for .torrent files, exporting the .torrent files, and running a
24 program designed to search the contents of the .torrent files is prohibited by the Court's
25 instruction that I "may not search for or view any other materials on the 'imaged' hard drive,
26

¹ <https://www.softpedia.com/get/Internet/Other-Internet-Related/Torrent-Hash-Extractor.shtml>.

1 including any items protected by attorney-client or work-product privilege.” Dkt. No. 182.
2 This is because the search would require me to view every .torrent file on Defendant’s hard
3 drive to determine if it matched the Exhibit A hashes, enabling me to view other BitTorrent
4 content that may exist on Defendant’s hard drive, which is specifically prohibited by the
5 Court’s Order.

6 16. The Order also prohibits me from confirming the owner/user of the hard drive
7 in question. To explain, to conduct a computer forensic examination of a device in a
8 BitTorrent copyright infringement case, I first attempt to confirm the user/owner of the hard
9 drive in question. I do this so that the discovery of evidence (or lack of evidence) is attributed
10 to the correct party. Therefore, even if I examined the hard drive in question using my
11 methodology outlined above, and the device contained no evidence of infringement or
12 destruction of evidence, I still would not be able to conclude that *Defendant’s* hard drive did
13 not contain such evidence. This is because I was not permitted to locate evidence confirming
14 Defendant’s ownership of the device.

15 17. Finally, the Court’s Order, as written, prohibits me from determining if anti-
16 forensic software was employed to avoid detection of the infringing files. This includes the
17 use of wiping software. To explain, the Order states that the examination “shall be limited to
18 searching for existing and/or deleted files matching the hash values[.]” Dkt. No. 182.
19 However, the existence of remnants of deleted files containing the hash values is not the only
20 method of establishing file deletion. Indeed, file deletion is also established by determining
21 if the hard drive has been wiped. When a defendant wipes his hard drive, there are likely no
22 remnants of deleted files. However, I would be able to determine that data destruction took
23 place by searching the hard drive’s registry for dates of significant events such as an operating
24 system’s installation date, Windows event logs, software installation dates, or files
25 evidencing the use of (and running) of software designed to wipe a hard drive. From my
26 experience examining hard drives in file sharing cases, one of the most common forms of

1 data destruction is when a defendant wipes his hard drive. Based on the Order, I was unable
2 to conduct this examination.

3
4 **DECLARATION**

5 **PURSUANT TO 28 U.S.C. § 1746**, I hereby declare under penalty of perjury that
6 the foregoing is true and correct.

7 Executed on this 28th day of October, 2019 at West Palm Beach, Florida.

8
9 By: 

10 **PATRICK PAIGE**
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

EXHIBIT A

Curriculum Vitae**Patrick L. Paige****8461 Lake Worth Road Suite 233G****Lake Worth, FL 33467****Main: 561.404.3074****Patrick@computerforensicsllc.com****<http://www.ComputerForensicsLLC.com>****Summary of Experience**

I have more than 25 years of law enforcement investigation experience, including more than 10 years as a computer crimes detective. I have performed computer forensic examinations for the Palm Beach County Sheriff's Office and surrounding cities, FBI, U.S. Customs, FDLE, Secret Service, ATF, and was a member of the South Florida ICAC taskforce for 10 years. In 2009 I was assigned to supervise the law enforcement operations for the Palm Beach County Sexual Predator Enforcement (SPE) at the located in Boca Raton FL. I have extensive knowledge of undercover online investigations including online enticement and Peer-to-Peer networks. I have been involved with hundreds of cases and have testified in State, Federal, Appellate, and Military courts as a computer expert including testifying as an expert in the functionality of Encase® at a murder trial. I have many forensic certifications including EnCE, and SCERS, additionally I was an EnCase® certified instructor for Guidance Software and have taught many forensic analysts around the country. I have earned many awards including Detective of the Month, U.S. Customs Service Unit Commendation Citation Award for computer forensic work, and have twice earned the Outstanding Law Enforcement Officer of the Year citation awarded by the United States Justice Department.

Computer Expert Witness Experience

During my tenure as a law enforcement officer and in private practice, I have been called to testify as an expert on numerous occasions in the field of computer forensics in Federal Courts in FL, CA, NJ, PA, IN, and NY, Appellate Courts, State Courts, and Military courts. The following is a list of cases I assisted in or have testified, either at trial or by deposition.

Strike 3 Holdings, LLC v. John Doe subscriber assigned to IP Address 73.225.38.130, U.S. District Court Western District of Washington, Civil Action, CASE No. 2:17-cv-01731-TSZ – June 27, 2019

Testimony: Deposition, IP detection software testing relating to BitTorrent.

Circuit Court of the 11th Judicial Circuit of Miami Dade County, Schmitz Development Company v. Dorothy Joan Schmitz, Case No. 2018-000931 CA (44) – April 24, 2019

Testimony: Evidentiary hearing before Judge Thomas relating to computer forensic examination and spoliation of evidence.

U.S District Court Southern District of Florida, Hayes Healthcare Services LLC, Hayes Medical Staffing LLC v. Chase Meacham, CASE No. 0:19-cv-60113-JIC – January 28, 2019

Testimony: Hearing in front of Judge Cohn relating computer forensic protocol and procedures.

Circuit Court of the 17th Judicial Circuit of Broward County, Doris Hamaway MD & Bridget Silva MD PA v. Bridget Silva MD, Case No. CACE17020169 – September 5, 2018

Appointment: Appointed by Judge Tuter as a neutral expert to server as an office of the court for the purpose of imaging, review and production of certain ESI requests and to protect attorney-client work product.

U.S District Court Southern District of Florida, CASE NO. 17-CV-61937, Federal Trade Commission v. Student Debt Doctor, LLC, a Florida corporation – October 2, 2017

Appointment: Appointed by the federal court ordered receiver Robert Carey, Esq. to oversee all the computer forensic imaging and data recovery of company servers. Work with investigators to secure company domains and locate company assets.

Estate of Aida Marie Gonzalez v. Delray Medical Center, INC. d/b/a Fair Oaks Pavilion, Praturi Sharma, MD, Miguel W. Mandoki, MD, The Chrysalis Center, Inc. Miriam R. Davis, LMHC; Antonio De Filippo, MD, Circuit Court of the 15th Judicial Circuit of Palm Beach County, Civil Division, Case No. 2014CA014731 AH – November 2, 2016

Testimony: Hearing in front of Judge Small relating to the processes involved in conducting computer forensic examination.

Circuit Court of the 17th Judicial Circuit of Broward County, State of Florida v. Richard Taffee, Criminal Division, Case No. 14006795CF10A – August 25, 2016

Testimony: Hearing in front of Judge Bidwill regarding Cellebrite's cell phone forensic hardware and the reports it produces.

U.S District Court Southern District of Florida, CASE No. 9:16-cv-80060-MARRA, PROJECT INVESTORS, INC. d/b/a CRYPTSY, a Florida corporation – May 6, 2016

Appointment: Appointed by the federal court ordered receiver James D. Sallah, Esq. to oversee all the computer forensic imaging and data recovery of company servers. Oversee and recover numerous cryptocurrency wallets from company servers.

Malibu Media, LLC v. John Doe, U.S. District Court Southern District of New York, Civil Action, CASE No. 1:14-cv-03504-JFB-SIL – April 20, 2016

Testimony: Hearing in front of Judge Steven I. Locke regarding BitTorrent testing and software.

Malibu Media, LLC v. John Doe, U.S. District Court Southern District of New York, Civil Action, CASE No. 1:14-cv-10151-KBF – November 12, 2015

Testimony: Deposition, Computer forensic examination findings & BitTorrent.

Malibu Media, LLC v. Tashiro, U.S. District Court Southern District of Indiana, Civil Action, CASE No. 1:13-cv-00202-WTL-MJD – April 30, 2015

Testimony: Evidentiary hearing in front of Judge Dinsmore regarding spoliation of evidence, computer forensic examination of digital evidence and matters relating to BitTorrent.

Malibu Media, LLC v. John Doe subscriber assigned to IP Address 24.14.81.195, U.S. District Court Northern District of Illinois, Civil Action, CASE No. 1:13-cv-006312 – February 17, 2015

Testimony: Deposition, Computer forensic examination findings & BitTorrent.

U.S District Court Southern District of Florida, CASE No. 14-cv-60468-MIDDLEBROOKS/BRANNON, Securities and Exchange Commission v. JCS Enterprises, Inc., d/b/a JCS Enterprises Services, Inc., T.B.T.I. Inc. – April 7, 2014

Appointment: Appointed by the federal court ordered receiver James D. Sallah, Esq. to oversee all the computer forensic imaging and data recovery of company computers. Assist federal prosecutors and defense council in the search and production of email. Search and production of financial data to forensic accountants.

Malibu Media, LLC v. Michael Harrison, U.S. District Court Southern District of Indiana, Civil Action, CASE No. 1:12-cv-01117-WTL-MJD – December 18, 2014

Testimony: Evidentiary hearing in front of Judge Dinsmore regarding spoliation of evidence, computer forensic examination of digital evidence and matters relating to BitTorrent.

Malibu Media, LLC v. Michael Harrison, U.S. District Court Southern District of Indiana, Civil Action, CASE No. 1:12-cv-01117-WTL-MJD – December 10, 2014

Testimony: Deposition, Computer forensic & BitTorrent.

Salvador Lopez Collazo and his wife Angelica Lopez Lopez, Plaintiffs VS. FEDEX GROUND PACKAGE SYSTEMS, INC., and BRUTIS TRUCKING, INC. and DAVID JAMES WIDELL, Defendants. Circuit Court of the Thirteenth Judicial Circuit in and for Hillsborough County, Florida Civil Division Case No. 12-018873 – April 8, 2014

Testimony: Deposition, cell phone forensics.

Restoration Management, Inc. v. James & Dana Pelletier, et al Eleventh Judicial Circuit of Florida Office of the General Magistrate before Magistrate Judge Schwabedessien Case No. 09-52134CA40 – November 4, 2013

Testimony: Expert testimony regarding forensic procedures involving QuickBooks software in the area of database files and program feature including audit trail.

State of Florida v. Michael Render, Second Judicial Circuit Leon County, FL Motion to Suppress Hearing Case No. 2011 CF 3514 – July 30, 2013

Testimony: Expert testimony regarding police procedures on conducting online investigations including peer2peer undercover operation. Computer forensics regarding peer2peer file sharing programs and how they work.

Malibu Media, LLC v. JOHN DOES 1, 6, 13, 14, and 16, U.S. District Court Eastern District of Pennsylvania, Civil Action No. 2012-2078 Consolidated from Cases: 2:12-cv-02078-MMB, 2:12-cv-02078-MMB, 5:12-cv-02088-MMB – June 10, 2013

Testimony: Expert testimony of my findings of the computers used by defendant Doe 16. Matters relating to the software used by IPP International, Germany to monitor and identify copyright infringers.

Malibu Media, LLC v. JOHN DOES 1, 6, 13, 14, and 16, U.S. District Court Eastern District of Pennsylvania, Civil Action No. 2012-2078 Consolidated from Cases: 2:12-cv-02078-MMB, 2:12-cv-02078-MMB, 5:12-cv-02088-MMB – May, 2013

Testimony: Evidentiary hearing in front of Judge Baylson via video, regarding spoliation of evidence, computer forensic examination of digital evidence and matters relating to BitTorrent.

Cypress Capital Group, Plaintiff v. Michael G. Blackmon, Defendant, Circuit of the Fifteenth Judicial Circuit, in and for Palm Beach County, Florida - Case No: 502008CA033553MB – July 20, 2011

Testimony; Deposition, labor dispute.

United States v. Michael Faxon, United States District Court, S.D. Florida, Fort Pierce Division – Case No. 09-14030-CR – February 5, 2010

Testimony; Forensic examination on the defendants' computer. Explained how the Defendant's computers was using peer-to-peer file sharing software known as LimeWire and GigaTribe.

United States Court of Appeals, Ninth Circuit. No. 07-10288.

United States of America, Plaintiff-Appellee, v. Walter M. SCHALES, Defendant-Appellant. - Argued April 15, 2008. - October 20, 2008

Testimony: Detective Paige of the Palm Beach County Sheriff's Office also testified that he recognized images on the CD-ROM depicting a child and an adult male that he arrested. The minor female depicted was five years old at the time of the photograph.

United States v. Kenneth WILK, U.S. District Court Southern District of Florida, Broward, Case No. 0:04-cr-60216-JIC – 2007. Capital Punishment Trail for Murder

Court: Testimony surrounding the intricate workings of Guidance's software EnCase®. EnCase is one of the top forensics software utilized by forensics analysts throughout the world.

United States Court of Appeals, Eleventh Circuit. No. 02-16809

United States of America, Plaintiff-Appellee, v. Samuel Alan MORTON, Defendant-Appellant. - April 01, 2004

Testimony: The government next called Patrick Paige, a detective with the Palm Beach County Sheriff's Office. Paige testified that he created a forensics report regarding the material on Morton's computer hard drive. Included in the report were downloaded movies that contained teen sex and a minor female and adult male engaged in sexual conduct. Paige also testified that he found approximately 30 images of minors. On re-direct Paige testified that Morton had approximately 50-100 images in his AOL account.

Work Experience

Computer Forensics LLC

(2012 - Present)

I'm currently a managing member of Computer Forensics LLC. The company is committed to providing top quality service and knowledge in the E-Discovery, Computer Forensics fields.

Guidance Software (Creators of EnCase® Software)***9 Years (2003 - 2012)***

During the years listed was employed as an Instructor with Guidance Software. Guidance Software is the world leader in providing computer and enterprise investigation solutions. Founded in 1997 and headquartered in Pasadena, CA, Guidance Software Inc., has offices and training facilities in California, Virginia, Texas and the United Kingdom. My duties as Instructor were to instruct students in the use of computer forensic software EnCase® made by Guidance Software. I also instruct students in other aspects of computer forensics like identifying and collecting computer evidence, how computers work, storage of electronic data and how files are deleted to name a few. Students who have attended classes I've taught include all branches of the military, local, state and federal officers. I have also assisted in the collection of data in the field for the Professional Division of Guidance Software who was contracted by the Department of Justice in the Sprint/Nextel merger in 2005.

Palm Beach County Sheriff's Office***21+ Years Employed (Ex: 1989 - 2011)******Detective Computer Crimes Unit (2000 - 2011)***

2000 to present, I've been assigned to the Computer Crimes Unit. During my current assignment to the Computer Crimes Unit I've investigated numerous Internet and computer related crimes. I've conducted many undercover online investigations resulting in the arrests of individuals around the United States. I have been involved in numerous search warrants involving online and child pornography investigations. I conduct computer forensic examinations for the Palm Beach County Sheriff's Office as well as local Law Enforcement. I've also done computer forensic examinations for the Broward County Sheriff's Office, FBI, U.S. Customs, FDLE, Secret Service, ATF and local cities. I have been a member of the South Florida ICAC (Internet Crimes Against Children) taskforce since January 2001. As the Senior Computer Forensic Examiner for the Sheriff's Office I was assigned to train new computer forensic examiners assigned to the unit. I served as point of contact for 2 known series of child pornography maintained by NCMEC (National Center for Missing and Exploited Children).

In 2009 I was assigned to supervise the law enforcement operations for the Palm Beach County Sexual Predator Enforcement (SPE) located in Boca Raton FL with offices provided by the TLO Corp. The TLO facility housed the computer servers used by law enforcement around the world to conduct P2P (Peer to peer) investigations. My assignments were as follows:

- Supervise the Detectives assigned to the unit which consisted of 6 Online Investigators and 2 Computer Forensic Examiners.
- Conduct computer forensic analysis on computers seized by the unit and testify to the findings.
- Coordinate and supervise the execution of search warrants developed by Detectives assigned to the unit. Detectives assigned to the unit conducted undercover Online investigations and peer to peer investigation via commonly used file sharing programs like LimeWire, GigaTribe, eMule to name a few.
- Worked with TLO software engineers on developing and enhancing software tools used by law enforcement officers.
- Prepared weekly reports of statistics and arrests made by the unit which were distributed to the local Chiefs of Police.
- Order and maintain computer forensic equipment, computers and software.
- Responsible for maintaining and tracking of all computer evidence seized for examination.

Detective Fraud Unit (1999)

This unit conducts investigations of criminal conduct in violation of Florida Laws concerning property crimes, fraud, forgery, and computer crimes. While I was assigned to this unit I was tasked with investigating cases connected with the Internet.

Agent Organized Crime Unit (1997 - 1999)

I was assigned to the Tactical Unit of the Palm Beach Sheriff's Office for two (2) years. During my assignment, I assisted in long term investigations, surveillances, dignitary protection and was assigned to aid the FBI, DEA, ATF and local law enforcement in investigations. I was also assigned to aid the Secret Service in the protection of heads of state, Vice President and President of the United States when they entered Palm Beach County.

Road Patrol Officer (1989 - 1997)

While assigned to the Road Patrol Division of the Palm Beach County Sheriff's Office, I developed a practical working knowledge of conducting investigations, evidence handling, and search and seizure laws. I also served as a FTO (Field Training Officer) for 3 years and was responsible for training over 35 new deputies hired by the Sheriff's Office.

Delray Beach Police Department**3 Years Employed (Ex: 1986 - 1989)**

While assigned to the Delray Beach Police Department I mainly worked in the road patrol division. I also served as a FTO (Field Training Officer) for a year.

ADVANCED LAW ENFORCEMENT & COMPUTER FORENSICS TRAINING

1. Seized Computer Evidence Recovery Specialist (SCERS) Federal Law Enforcement training Center in Glynco, GA 80HRS (2/2001)
2. Investigations of Computer Crimes (The International Association of Chiefs of Police) 40HRS
3. EnCase® Intermediate Analysis & Reporting course (Guidance Software Inc.) 32HRS
4. EnCase® Expert Series Internet & E-mail Examination course (Guidance Software Inc.) 32HRS
5. Conducting Online ICAC Investigations (Law Enforcement Against Child Harm Taskforce) 40HRS
6. Investigating Computer Use of the Internet by Child Sex Offenders (Institute of Child Advocacy)
7. Advanced Sex Crimes Investigations course (Palm Beach Community College) 40HRS
8. Organized Crimes Investigations course (Palm Beach Community College) 40HRS
9. Field Training Officer course (Palm Beach Community College) 40HRS
10. Advance Narcotics Identification (Palm Beach Community College) 40HRS
11. Dignitary Protection Operations (Tactical Response Training) 32HRS
12. Forensic Computer Examiner Training Program (International Association of Computer Investigation Specialists - IACIS) 80HRS (5/2004)
13. 17th Annual Crimes Against Children Conference (Dallas, TX) 20HRS August 15-18, 2005
(Conference courses attended: Forensics on Portable Devices, AOL & Yahoo investigations, Email Tracing and Techniques for Investigating Wireless Devices.
14. 18th Annual Crimes Against Children Conference (Dallas, TX) 20HRS August 21-24, 2006
(Conference courses attended: Email and IP Tracing, Windows XP Forensic Gems, Digital Imaging Forensics and Investigating Wireless Devices.
15. CEIC 2012 (Computer and Enterprise Investigations Conference) 4 days (Summerlin, Nevada) May 21-24 2012
(Conference courses attended: EnCase® version 7 training updates, Using cloud computing in forensics and electronic discovery, Embedded EnScripts®, Forensic tracking of USB devices, TD2, TD3 and the future of the forensic duplicator, exFat forensics and revealing Windows® 7 artifacts.
16. CEIC 2015 (Computer and Enterprise Investigations Conference) 4 days (Las Vegas, Nevada) May 18-21 2015
Conference courses/labs attended:
 1. Investigating a User's Internet Activity Across Computers, Smartphones and Tablets.
 2. Tracking the Use of USB Storage on Windows 8 & Windows Shellbag Forensics in Depth.
 3. Investigating Exchange, Microsoft Cloud Services and Office 365.
 4. Tips and Tricks from Guidance Software Technical Services.
 5. Practical Python Forensics, Practical Python Forensics & Advanced Examination Reporting.
 6. Windows 8 - Deconstructing the Catalog and Other Artifacts.
17. Enfuse 2018 (Security, Digital Investigation and eDiscovery Conference) 3 Days (Las Vegas, Nevada) May 21-24 2018
Conference courses/labs attended:
 1. Digital Evidence from Social Networking Sites & Smartphone Apps.
 2. The future of EnCase.
 3. The Art & Science of Incident Response.
 4. The New Apple File System (APFS)

5. Customized Reports with EnCase.
6. The Bits behind the Coin: Following the Trail of a Cryptocurrency Investigation.
7. EnScript for Examiners & Index in EnCase software
8. Logical Imaging with Tableau TX1

AWARDS

Delray Beach Police Department

- 3 – Patrol Division Commendations.
 1987 – Rookie of the year.
 1988 – Police officer of the month for March and August.

Palm Beach County Sheriff's Office

- 1991 – Deputy of the year awarded by the 100 Men's Club of Boca Raton & Rotary Club.
 1997 – Deputy of the Month for June.
 2001 – Detective of the Month for October.
 2002 – Outstanding Law Enforcement Officer of the Year awarded by the United States Department of justice for work in the U.S. v Jerrold Levy case. [News Articles](#) Certificate of Achievement issued by the National Center for Missing & Exploited Children for work performed in the Levy case.
 2003 – U.S. Customs Service Unit Commendation Citation Award for computer forensic work in Operation Hamlet. Operation Hamlet was one of the largest rings in U.S. Customs history of individuals who were molesting their own children, and transmitting the images and video via the Internet. [News Articles](#) 2005 – Detective of Month for December.
 2006 – Letter of Commendation issued by the FBI for outstanding computer forensic work in the U.S. v Frank Grasso case. [Article](#)
 2007 – Outstanding Law Enforcement Officer of the Year awarded by the United States Department of Justice for work in the U.S. v Jimmy Oliver case. [Press Release](#)
 2009 – 20 Year Good Conduct Medal – For honorable and faithful service for a period of twenty years.
 2009 – 20 Year Honorable Service Medal – For exemplary conduct, efficiency and fidelity for a period of twenty years.

CERTIFICATIONS / MEMBERSHIPS

- EnCE – EnCase® Certified Examiner (Cert# 15-0703-1199 Exp. 7/21/2021)
 CEECS – Certified Electronic Evidence Collection Specialist – IACIS
 SCERS – Seized Computer Evidence Recovery Specialist – FLETC (Federal Law Enforcement Training Center in GA)
 CFCE – Certified Forensic Computer Examiner – IACIS – CFCE from 2005 to 2008
 Member of IACIS – International Association of Computer Investigative Specialists
 Member of MECTF – Miami Electronics Crimes Task Force hosted by the United States Secret Service

COURSES TAUGHT FOR GUIDANCE SOFTWARE

- 1) Intermediate Analysis & Reporting – Sterling, VA December 2nd – 5th 2003 (32 hrs)
- 2) Introductory Computer Forensics – Sterling, VA August 12th – 15th 2003 (32 hrs)
- 3) Introductory Computer Forensics – Sterling, VA September 16th – 19th 2003 (32 hrs)
- 4) Incident Response, Forensic Analysis & Discovery – Sterling, VA September 29th – October 3rd 2003 (40 hrs)
- 5) Introductory Computer Forensics – Sterling, VA January 6th – 9th 2004 (32 hrs)
- 6) Introductory Computer Forensics – Sterling, VA August 10th – 13th 2004 (32 hrs)
- 7) Introductory Computer Forensics – Sterling, VA June 28th – July 1st 2005 (32 hrs)
- 8) Intermediate Analysis & Reporting (Special Class for U.S. Military) – Sterling, VA October 16th – 20th 2006 (40 hrs)
- 9) EnCase® Computer Forensics II – Sterling, VA January 29th – February 4th 2007 (32 hrs)
- 10) EnCase® Computer Forensics I – Sterling, VA April 23rd – April 29th 2007 (32 hrs)
- 11) EnCase® Computer Forensics I – Sterling, VA September 11th – September 14th 2007 (32 hrs)

CERTIFICATE OF SERVICE

I, Annabel Barnes, hereby certify that on October 28, 2019, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system which will send notification of filing to the following parties:

Joshua L. Turnham, WSBA #49926
E-mail: joshua@turnhamlaw.com
THE LAW OFFICE OF JOSHUA L. TURNHAM PLLC
1001 4th Avenue, Suite 3200
Seattle, Washington 98154
Telephone: (206) 395-9267
Facsimile: (206) 905-2996

Attorneys for Non-Party Defendant's Son

F. Christopher Austin, Admitted Pro Hac Vice
Email: caustin@weidemiller.com
Allen Gregory Gibbs, Admitted Pro Hac Vice
Email: ggibbs@weidemiller.com
WEIDE & MILLER, LTD.
10655 Park Run Drive, Suite 100
Las Vegas, Nevada 89144
Telephone: (702) 382-4804

Derek A. Newman, WSBA #26967
Email: dn@newmanlaw.com
Rachel Horvitz, WSBA #52987
Email: rachel@newmanlaw.com
NEWMAN DU WORS LLP
2101 4th Avenue, Suite 1500
Seattle, Washington 98121
Telephone: (206) 274-2800
Facsimile: (206) 274-2801

*Attorneys for Third-Party Witnesses Tobias Fieser, IPP International UG,
Bunting Digital Forensics, LLC, Stephen M. Bunting*

Adrienne D. McEntee, WSBA #34061
Beth E. Terrell, WSBA #26759
Email: bterrell@terrellmarshall.com
amcentee@terrellmarshall.com
936 North 34th Street, Suite 300

1 Seattle, Washington 98103-8869
2 Telephone: (206) 816-6603
3 Facsimile: (206) 319-5450

4 J. Curtis Edmondson, WSBA #43795
5 Email: jcedmondson@edmolaw.com
6 EDMONDSON IP LAW
7 399 NE John Olsen Avenue Hillsboro
8 Oregon 97124
9 Telephone: (503) 336-3749

10 *Attorneys for Defendant*

11 DATED this 28th day of October 2019 at Seattle, Washington.

12 /s/ Annabel Barnes

13 Annabel Barnes
14
15
16
17
18
19
20
21
22
23
24
25
26